SQUAREFREE VALUES OF POLYNOMIALS OVER THE RATIONAL FUNCTION FIELD

ZEÉV RUDNICK

Abstract. We study representation of square-free polynomials in the polynomial ring $\mathbb{F}_q[t]$ over a finite field $\mathbb{F}_q$ by polynomials in $\mathbb{F}_q[t][x]$. This is a function field version of the well studied problem of representing squarefree integers by integer polynomials, where it is conjectured that a separable polynomial $f \in \mathbb{Z}[x]$ takes infinitely many squarefree values, barring some simple exceptional cases, in fact that the integers a for which $f(a)$ is squarefree have a positive density. We show that if $f(x) \in \mathbb{F}_q[t][x]$ is separable, of bounded degree and height, then as $q \to \infty$, for almost all monic polynomials $a(t)$, the polynomial $f(a)$ is squarefree.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of q elements. We wish to study representation of square-free polynomials in the polynomial ring $\mathbb{F}_q[t]$ by polynomials in $\mathbb{F}_q[t][x]$. This is a function field version of the well studied problem of representing squarefree integers by integer polynomials, where it is conjectured that a separable polynomial (that is, without repeated roots) $f \in \mathbb{Z}[x]$ takes infinitely many squarefree values, barring some simple exceptional cases, in fact that the integers a for which $f(a)$ is squarefree have a positive density. The case of $\deg f \le 2$ has been dealt with by a simple sieve argument [6]. For cubics, Erdös [1] showed that there are infinitely many squarefree values, and Hooley [3] gave the result about positive density. Beyond that nothing seems known unconditionally for irreducible f, for instance it is still not known that a^4+2 is infinitely often squarefree. Granville [2] showed that the ABC conjecture completely settles this problem.

In this note we study a function field version of this problem. Given a polynomial $f(x) = \sum_j \gamma_j(t)x^j \in \mathbb{F}[t][x]$ which is separable, that is with no repeated roots in any extension of $\mathbb{F}_q(t)$, we want to know how often is $f(a)$ squarefree in $\mathbb{F}_q[t]$ as a runs over (monic) polynomials in $\mathbb{F}_q[t]$.

For any field $\mathbb{F}$, let

$$M_n(\mathbb{F}) = \{a \in \mathbb{F}[t] : \deg a = n, a \text{ monic}\} \tag{1.1}$$

Date: December 17, 2012.

This work was conceived during the ERC Research Period on Diophantine Geometry in Pisa during September 2012.

The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement n° 320755.

so that $\#M_n(\mathbb{F}_q)=q^n$. Define

$$\mathcal{S}_f(n)(\mathbb{F})=\{a\in M_n(\mathbb{F}) : f(a) \text{ is squarefree }\} \tag{1.2}$$

and we want to study the frequency

$$\frac{\#\mathcal{S}_f(n)(\mathbb{F}_q)}{\#M_n(\mathbb{F}_q)} \tag{1.3}$$

in an appropriate limit.

There are two possible limits to take: Large degree ($n\to\infty$) while keeping the constant field $\mathbb{F}_q$ fixed, or large constant field ($q\to\infty$) while keeping n fixed.

The large degree limit (q fixed, $n\to\infty$) was investigated by Ramsay [5] who showed:

Theorem 1.1. *Assume $f\in\mathbb{F}_q[t][x]$ is separable and irreducible. Then*

$$\frac{\#\mathcal{S}_f(n)(\mathbb{F}_q)}{\#M_n(\mathbb{F}_q)}=c_f+O_{f,q}(\frac{1}{n}), \quad \text{as } n\to\infty$$

with

$$c_f=\prod_P(1-\frac{\rho_f(P^2)}{|P|^2}) ,$$

the product over prime polynomials P, and for any polynomial $D\in\mathbb{F}_q[t]$, $\rho_f(D)=\#\{C \bmod D : f(C)=0 \bmod D\}$. The implied constant depends on f and on the finite field size q. The density c_f is positive if and only if there is some $a\in\mathbb{F}_q[t]$ such that $f(a)$ is squarefree.

Ramsay actually counts all polynomials up to degree n, and does not impose the monic condition. See also Poonen [4] for multi-variable versions.

Ramsay's theorem is proved by an elementary sieve argument, with one crucial novel ingredient due to Elkies to deal with the contribution of large primes to the sieve, which is completely unavailable in the number field case; in Granville's work [2], the ABC conjecture plays an analogous rôle.

In this note we deal with the large finite field limit, of $q\to\infty$ while n is fixed. Here it makes little sense to fix the polynomial f, so we also allow variable f, as long as restrict the degree (in x) and height, where for a polynomial $f(x,t)=\sum_j\gamma_j(t)x^j\in\mathbb{F}[t][x]$, the height is $\operatorname{Ht}(f)=\max_j\deg\gamma_j(t)$. We will show

Theorem 1.2. *For all separable $f\in\mathbb{F}_q[t][x]$, as $q\to\infty$,*

$$\frac{\#\mathcal{S}_f(n)(\mathbb{F}_q)}{\#M_n(\mathbb{F}_q)}=1+O(\frac{(n\deg f+\operatorname{Ht}(f))\deg f}{q}) , \tag{1.4}$$

the implied constant absolute.

Thus if we fix n, the degree and the height, as $q\to\infty$ for almost all $a\in M_n(\mathbb{F}_q)$ the polynomials $f(a)$ are squarefree. For instance, the number of $a(t)\in M_n(\mathbb{F}_q)$ for which $a(t)^4+2$ is squarefree is, for q odd, $q^n+O(nq^{n-1})$.

Remark: It is possible to have separable f with no squarefree values, for instance take

$$f(x) = \prod_{\alpha,\beta\in\mathbb{F}_q} (x - \alpha t - \beta) = x^{2q} + \dots \ . \tag{1.5}$$

Then for all $a \in \mathbb{F}_q[t]$, $f(a)$ is divisible by $(\prod_{\gamma\in\mathbb{F}_q}(t-\gamma))^2 = (t^q - t)^2$. Indeed, if we fix $\gamma \in \mathbb{F}_q$, any $a \in \mathbb{F}_q[t]$ is congruent modulo $(t-\gamma)^2$ to some $\alpha t + \beta$ and hence $f(a) \equiv f(\alpha t + \beta) = 0 \bmod (t-\gamma)^2$. Thus we need to impose some restriction on the degree of f in Theorem 1.2.

Theorem 1.2 is a consequence of a purely algebraic result, valid over *any* field $\mathbb{F}$.

Theorem 1.3. *If $f \in \mathbb{F}[t][x]$ is separable over $\mathbb{F}(t)$ then $\mathcal{S}_f(n)(\mathbb{F})$ is the complement of a $\underline{\text{proper}}$ Zariski-closed hypersurface of the affine n-dimensional space $M_n(\mathbb{F})$, of degree $D \le 2(n \deg f + \operatorname{Ht} f)\deg f$.*

Indeed, Theorem 1.3 implies that the number of $a \in M_n(\mathbb{F}_q)$ for which $f(a)$ is not squarefree is at most Dq^{n-1}, where D is the total degree of an equation defining the hypersurface. This is an elementary fact, seen by fixing all variables but one (cf [7, §4, Lemma 3.1]).

2. Proof of Theorem 1.3

We write

$$f(x,t) = \gamma_0(t) + \gamma_1(t)x + \cdots + \gamma_\ell(t)x^\ell \tag{2.1}$$

with $\gamma_j(t) \in \mathbb{F}[t]$, and $\gamma_\ell(t) \ne 0$. Denote by

$$\Delta_f(t) = \operatorname{disc}_x f(x,t) \tag{2.2}$$

the discriminant of $f(x)$ as a polynomial of degree ℓ with coefficients in $\mathbb{F}[t]$; it is a universal polynomial with integer coefficients in $\gamma_0(t), \dots, \gamma_\ell(t)$:

$$\Delta_f(t) = \operatorname{Poly}_{\mathbb{Z}}(\gamma_0(t), \dots, \gamma_\ell(t)) \in \mathbb{F}[t] \ . \tag{2.3}$$

Separability of f (over $\mathbb{F}(t)$) is equivalent to the discriminant not being the zero polynomial: $\Delta_f(t) \ne 0$.

The key observation is that $f(a) \in \mathbb{F}[t]$ being squarefree is equivalent to requiring that the polynomial $t \mapsto f(a(t),t)$ does not have any multiple zeros (in any extension of the field $\mathbb{F}$). This is in fact a polynomial condition, that is a polynomial system of equations for the coefficients $a_0, a_1, \dots a_{n-1}$ of $a(t) = a_0 + a_1 t + \cdots + a_{n-1}t^{n-1} + t^n$ which is given by the vanishing of the discriminant:

$$\operatorname{disc} f(a(t),t) = 0 \ . \tag{2.4}$$

It suffices to show that this equation defines a *proper* hypersurface.

Before doing so, we bound the degree D of the hypersurface (2.4): For $f(x,t)$ as in (2.1), $f(a(t),t)$ is a polynomial in t of degree

$$\deg f(a(t),t) \le n \deg f + \max \deg \gamma_j = n \deg f + \operatorname{Ht}(f) \ . \tag{2.5}$$

The coefficients are polynomials in the a_j of degree at most $\deg f$. Now the discriminant of a polynomial $\sum_{j=0}^{m} h_j t^j$ is homogeneous in the coefficients h_j of degree $2m-2$. Hence $a \mapsto \operatorname{disc} f(a(t),t) = \sum_k \delta_k \prod a_i^{k_i}$ has total degree at most $D = 2(n \deg f + \mathrm{Ht}(f)) \deg f$. It remains to show that the equation is nontrivial.

The condition that the polynomial $f(a(t))$ has multiple zeros is that there is some $\rho \in \overline{\mathbb{F}}$ (an algebraic closure of $\mathbb{F}$) with

$$f(a(\rho),\rho) = 0, \quad \frac{\partial f}{\partial x}(a(\rho),\rho) \cdot a'(\rho) = 0\ . \tag{2.6}$$

This system breaks up into the union of two systems: The singular case

$$f(a(\rho),\rho) = 0, \quad \frac{\partial f}{\partial x}(a(\rho),\rho) = 0 \tag{2.7}$$

and the generic case

$$f(a(\rho),\rho) = 0, \quad a'(\rho) = 0\ . \tag{2.8}$$

In the singular case (2.7), ρ is a zero of the discriminant $\Delta_f(t)$, which is not identically zero (since we assume f is separable) and hence there are only finitely many possibilities for such ρ. Given one of those ρ, let β_j be one of the at most $\deg f$ multiple zeros of $f(x,\rho)$, then we need $a(t)$ to satisfy $a(\rho) = \beta_j$, i.e.

$$a_0 + a_1\rho + \cdots + a_{n-1}\rho^{n-1} + \rho^n = \beta_j \tag{2.9}$$

which is a (non-degenerate) linear equation, and therefore carves out an $n-1$-dimensional subspace of a's. Thus the singular locus (2.7) consists of at most finitely many hyperplanes, and hence if non-empty has dimension $n-1$.

To study the generic case (2.8), we define

$$W = \{(\rho,\vec{a}) \in \mathbb{A}^1 \times \mathbb{A}^n : (2.8) \text{ holds}\}\ . \tag{2.10}$$

We have a fibration of W over the ρ line $\mathbb{A}^1$ and a map $\phi : W \to \mathbb{A}^n$, the restriction of the projection $\mathbb{A}^1 \times \mathbb{A}^n \to \mathbb{A}^n$,

$$\begin{tikzcd} & W \subset \mathbb{A}^1 \times \mathbb{A}^n \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\ \mathbb{A}^1 & & \mathbb{A}^n \end{tikzcd} \tag{2.11}$$

and the solutions of (2.8) are precisely $\phi(W)$.

The equation $a'(\rho) = 0$ is the condition

$$a_1 + 2\rho a_2 + \cdots + (n-1)\rho^{n-2} a_{n-1} + n\rho^{n-1} = 0 \tag{2.12}$$

and allows us to solve for a_1 in terms of the other $n-1$ coefficients and substitute in the equation $f(a)(\rho) = 0$ from (2.8) to get a single polynomial equation for $a_0, a_2, \ldots, a_{n-1}$. For ρ such that this equation is not identically zero, we get a codimension one condition. We will show that there are at most $\deg \gamma_\ell$ points ρ such that this equation is identically zero.

In fact using (2.12) we can write

$$a(\rho) = a_0 - \rho^2 a_2 - 2\rho^3 a_3 - \cdots - (n-2)\rho^{n-1}a_{n-1} - (n-1)\rho^n \tag{2.13}$$

and so if $f(x) = \gamma_0(t) + \gamma_1(t)x + \cdots + \gamma_\ell(t)x^\ell$ then we get

$$\begin{aligned}\gamma_0(\rho) + \gamma_1(\rho)(a_0 - \rho^2 a_2 - 2\rho^3 a_3 - \cdots - n\rho^n) + \dots \\ + \gamma_\ell(\rho)(a_0 - \rho^2 a_2 - 2\rho^3 a_3 - \cdots - n\rho^n)^\ell = 0\end{aligned} \tag{2.14}$$

which is of degree $\le \ell$ in a_0, and the coefficient of a_0^ℓ is $\gamma_\ell(\rho)$. Hence if ρ is not one of the $\deg \gamma_\ell$ zeros of $\gamma_\ell(t)$ (which is not the zero polynomial), the equation is nonzero and the fiber $\pi^{-1}(\rho)$ has dimension $n-2$.

In addition, there are the at most $\deg \gamma_\ell$ exceptional fibers where the equation may vanish, and each of these fibers has dimension $n-1$.

Therefore we see that $\dim W = n-1$. Since the set Z of a's which fall into the generic case are precisely $Z = \phi(W)$, it follows that $\dim Z \le n-1$.

This concludes the proof of Theorem 1.3.

References

[1] P. Erdös. *Arithmetical properties of polynomials.* J. London Math. Soc. 28, (1953). 416–425.

[2] A. Granville, *ABC allows us to count squarefrees.* Internat. Math. Res. Notices 1998, no. 19, 991–1009.

[3] C. Hooley, *On the power free values of polynomials.* Mathematika 14 1967 21–26.

[4] B. Poonen, *Squarefree values of multivariable polynomials.* Duke Math. J. 118 (2003), no. 2, 353–373.

[5] K. Ramsay, *Square-free values of polynomials in one variable over function fields.* Internat. Math. Res. Notices, no. 4 (1992) 97–102.

[6] G. Ricci, *Ricerche aritmetiche sui polinomi.* Rend. Circ. Mat. Palermo 57 (1933), 433–475.

[7] Wolfgang M. Schmidt, Equations over finite fields: an elementary approach. Second edition. Kendrick Press, Heber City, UT, 2004

Raymond and Beverly Sackler School of Mathematical Sciences, Tel Aviv University, Tel Aviv 69978, Israel

E-mail address: rudnick@post.tau.ac.il